

Written Testimony of Orin S. Kerr
Associate Professor, George Washington University Law School
For the House Judiciary Committee
Subcommittee on the Constitution
May 20, 2003

Mr. Chairman and members of the Subcommittee, my name is Orin S. Kerr, and I am an Associate Professor at George Washington University Law School. I am grateful for the opportunity to appear before you today to discuss Internet surveillance law and the effect of the USA Patriot Act.

My testimony will focus on the controversial pen register amendments to the Patriot Act, found in Section 216 of the Act. As you know, these amendments have received a great deal of criticism. Critics have claimed that the amendments gave the government unprecedented powers to wiretap the Internet. I believe that these criticisms are misplaced. They are based on a misunderstanding of how the complex laws governing Internet surveillance interact with each other. When properly understood, the Patriot Act's provisions applying the pen register law to the Internet appear instead as an important first step toward modernizing the surveillance laws and protecting privacy in the Internet age. The pen register amendments to the Patriot Act are not so much part of the problem as they are an initial step toward a solution that will best balance the protection of privacy and the needs of law enforcement. In my testimony this afternoon, I will explain why I believe this is true. I will then suggest two additional steps that I believe Congress should take to develop this area of law in the future.

Before I begin, let me note that my testimony this afternoon is a streamlined version of an argument I made in a recent law review article. Those wishing to read more can look at the full article, "Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't." The article appears in the Winter 2003 issue of the *Northwestern University Law Review*, and it covers the pen register laws, the use of Carnivore, and the new computer trespasser exception to the Wiretap Act. A .pdf copy of the article can be downloaded for free from the Internet at this address: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=317501.

To begin understanding the effect of the Patriot Act's pen register amendments, it helps to start with some history. The surveillance laws that apply to the Internet were originally designed to apply to the telephone network. Telephone network surveillance is governed by two complementary laws: the Wiretap Act, enacted in 1968 and codified at 18 U.S.C. §§ 2510-22; and the Pen Register Statute, enacted in 1986 and codified at 18 U.S.C. §§ 3121-27. These two laws govern real-time surveillance of the telephone network in criminal investigations. The laws coexist because they cover different things: the Wiretap Act protects the "contents" of communications with a very high degree of privacy protection, and the Pen Register statute protects non-content addressing information with a lesser degree of privacy protection. This bifurcation between contents and non-content addressing information is consistent with and follows from the Supreme Court's cases interpreting how the Fourth Amendment applies to the telephone network. In *Berger v. New York*,

388 U.S. 41 (1967), the Supreme Court held that the Fourth Amendment protected the contents of telephone calls, whereas in *Smith v. Maryland*, 442 U.S. 745 (1979), the Supreme Court held that the Fourth Amendment does not protect non-content information relating to telephone calls such as might be collected by a pen register device, which was an early machine used to record the numbers dialed from a telephone.

The line between the Wiretap Act and the Pen Register statute is easy to understand for a traditional telephone call. If I place a phone call, the actual conversation between the person I call and myself are the “contents” of the call. If the government wishes to listen in on the call, the privacy protections of the Wiretap Act prohibit the government from doing so unless the government first obtains a Wiretap Order, which is a type of “super” search warrant. In contrast, information about the call such as my phone number, the time I called, the duration of the call, and the number I dialed is the non-content addressing information about the call. This information is protected by the Pen Register statute but not the Wiretap Act. If the government wishes to have the phone company record this information and disclose it to the government, the privacy protections of the Pen Register statute prohibit this unless the government first obtains a pen register order. A pen register order is a “relevance” court order; the government can obtain such an order if the information to be collected is relevant to an ongoing criminal investigation. The basic rule is that the lesser privacy protections of the Pen Register statute apply to non-content information, and the greater privacy protections of the Wiretap Act apply to content information.

Now let’s turn from the telephone network to the Internet. In 1986, Congress enacted the Electronic Communications Privacy Act, also known as “ECPA.” ECPA established that the Wiretap Act that protects the contents of telephone calls also protects the contents of Internet communications. ECPA also created a new privacy law known as the Stored Communications Act, codified at 18 U.S.C. §§ 2701-11, which created statutory privacy protection for stored Internet communications such as stored e-mails. However, ECPA left a very important question unclear: what privacy protection if any applied to real-time surveillance of non-content addressing information for Internet communications? What law governs the real-time surveillance of Internet packet headers or e-mail headers-- non-content addressing information that is the Internet equivalent of the outside envelope of a postal letter or the addressing information for a telephone call? The Pen Register statute that already protected equivalent information for telephone calls provided the obvious source of privacy protection, but its scope was unclear. As enacted in 1986, parts of the Pen Register statute appeared to apply broadly to protect both telephone and Internet communications. However, other parts of the statute seemed narrowly drafted to apply only to the telephone. These mixed signals left the scope of the Pen Register statute unclear. The text of the 1986 Act simply failed to answer whether the Pen Register statute protected the privacy of non-content Internet communications in the same way it protected the privacy of non-content telephone communications.

The uncertain scope of the Pen Register statute created a complicated situation for law enforcement before the enactment of the Patriot Act. The applicable law looked quite different depending on whether one assumed that the Pen Register law applied to the Internet. If the Pen Register statute did apply to the Internet, then the law prohibited the government from monitoring

non-content information on the Internet without a pen register court order. It also made it a crime for private parties or foreign governments to conduct such surveillance. At the same time, the law would then authorize the government to conduct non-content surveillance (or order an Internet service provider to conduct such surveillance on the government's behalf) by obtaining a pen register order. If the Pen Register law did not protect the privacy of Internet communications, however, then no privacy law at all protected non-content information of Internet communications in transit. The government would be able to install Internet wiretapping devices such as "Carnivore" without any court order or any judicial review so long as the device did not collect any contents and was therefore exempt from the Wiretap Act. Any private citizen or foreign government would have been able to do the same. At the same time, the law would have left unclear what authority the government would be able to use to compel an Internet service provider to conduct such surveillance on the government's behalf.

In the period before the Patriot Act, the Department of Justice concluded that on balance the better argument was that the Pen Register statute did apply to the Internet. In other words, DOJ concluded that the law protected the privacy of Internet communications and required the government to obtain a court order before it could conduct real-time surveillance of non-content information on-line. Federal prosecutors routinely obtained pen register orders from magistrate judges in Internet crime investigations. While magistrate judges occasionally expressed initial concern over whether the Pen Register statute in fact applied to the Internet, every federal magistrate judge except one concluded that the statute did apply to the Internet and approved the government's application for the court order. The one magistrate judge who disagreed was located in San Jose, California. In an unpublished order in November 2000, this particular judge denied the government's *ex parte* application for a pen register order on the ground that the Pen Register statute did not apply to the Internet, but rather applied only to the telephone network.

Section 216 of the Patriot Act clarified that the Pen Register statute did in fact protect the privacy of Internet communications. It replaced the telephone-specific language from the 1986 Act with broader, technology-neutral language: the new version of the Pen Register statute protects any real-time non-content "dialing, routing addressing, or signaling information" relating to either telephone or Internet communications. In practice, this amendment maintained the status quo: it permitted the Justice Department to continue its pre-Patriot Act procedures. How much the change altered existing law in a formal sense depends upon whether you conclude that the Pen Register law applied to the Internet before the Patriot Act. If you believe that the Pen Register law did already apply, then the amendment merely clarified existing law. If you believe that it did not, the amendment extended the privacy protection of the Pen Register statute to the Internet.

I believe this amendment was a positive step forward that would have won widespread support if it had been better understood at the time of the Patriot Act's passage. The amendment expanded the scope of a privacy law, making sure that the government needed a court order where before it was possible that no court order was necessary. Why did this provision trigger such controversy? One reason is that many commentators incorrectly believed that the Pen Register amendments lessened the protections of the companion Wiretap Act. Many commentators wrongly

assumed that before the Patriot Act, the Wiretap Act had protected both contents and non-content information. Based on that incorrect assumption, they concluded that the Pen Register amendments lessened privacy protections by moving the protection of non-content information from the high privacy protections of the Wiretap Act to the lower protections of the Pen Register statute. This led to widely-reported claims that the Pen Register amendments gave the government unprecedented new powers to wiretap the Internet without a probable cause search warrant.

The premise is mistaken, however. The Wiretap Act protects only the contents of communications; it does not protect non-content information. This was true both before and after the Patriot Act. The Patriot Act did not change the scope of the Wiretap Act's protection of contents; it left unchanged the statutory definition of "contents" in 18 U.S.C. § 2510(8) that has existed since 1986. To the extent the pen register amendment of the Patriot Act changed the law at all, it increased the scope of privacy protections by making sure that non-content information was not left unprotected by federal privacy law. This did empower the government to obtain court orders in Internet crime investigations under the low pen register standard: as is always the case with laws regulating surveillance, the power to seek a court order to conduct the surveillance is an exception to the law that applies when the law regulates the surveillance. But the pen register amendment did not lessen the protections of the Wiretap Act. Instead it clarified that the same rules apply to the Internet that have traditionally applied to the telephone.

I stated at the beginning of my testimony that the pen register amendments of the Patriot Act were an important first step toward modernizing the Internet surveillance laws and protecting privacy. This raises the question, what steps remain? I think there are two areas that should demand Congress's attention in the future.

First, Congress should clarify the line between "contents" protected by the Wiretap Act and "dialing, routing, addressing, and signaling information" protected by the Pen Register statute. Today we know that human-to-human communications such as the body and the subject lines of e-mails count as "contents." We also know that computer-to-computer communications such as Internet Protocol packet headers count as "dialing, routing, addressing, and signaling information." However, we don't know how human-to-computer communications are treated under current law. Just two weeks ago, one court suggested that search terms entered into Internet search engines are contents protected by the Wiretap Act. *See In re Phormatrak, Inc. Privacy Litigation*, -- F.3d --, 2003 WL 21038761 (1st Cir. May 9, 2003). Three years ago, another court indicated that passwords entered into computers are also contents protected by the Wiretap Act. *See United States Telecom Ass'n v. FCC*, 227 F.3d 450, 462 (D.C. Cir. 2000). However, the absence of a statutory suppression remedy in the Internet surveillance laws means that these decisions appear only sporadically in unusual civil contexts, and tend to have uncertain scope. Congress should either add a statutory suppression remedy that will have the effect of empowering the courts to clarify the line between the two statutes in criminal cases, or should take steps to clarify that line itself.

Second, I believe that Congress should raise the standard that the government needs to satisfy to obtain a pen register court order. First, the factual threshold should be raised from mere relevance

to "specific and articulable facts," matching the protection that exists under current law for stored non-content records. *See* 18 U.S.C. § 2703(d). Second, the current certification standard should be replaced with judicial review. Current law states that the government lawyer applying for a pen register order must certify that the factual threshold has been satisfied, and requires the magistrate judge to grant the application if the certification has been made. The law should be changed so that magistrate judges evaluate whether the government's application satisfies the factual showing. Again, this matches the protection that exists under current law for stored non-content records. The added judicial review will provide the public a greater assurance that the law is not being abused, whether in the telephone context or the Internet context. At the same time, based on my experience as a federal prosecutor I believe that the slightly higher threshold will not create a substantial burden for law enforcement.

Let me conclude by offering a few thoughts on the big picture. Today the law of Internet surveillance in criminal investigations remains governed primarily by the Electronic Communications Privacy Act of 1986. Congress has amended this law several times since 1986, including when it passed the USA Patriot Act, but the basic framework of the 1986 law remains in place. The 1986 Act was a remarkable achievement for its day: it protected the privacy of Internet communications long before most Americans had even heard of the Internet. Even today, the law remains surprisingly workable and effective. The 1986 Act left many questions unresolved, however. The fast pace of technological change raises the bar as well; developments such as the World Wide Web require us to fit new technologies into old laws. As a result, the Internet surveillance laws demand constant legislative attention both to address existing problems latent in the 1986 statutory scheme and to address new difficulties raised by technological change.

Fortunately, the provisions of the USA Patriot Act that relate to Internet surveillance in criminal investigations are much more balanced than many have feared. Much of the media coverage surrounding provisions such as the pen register amendments failed to appreciate the complex inner workings of the law, and as a result tended to misrepresent the effect of the Patriot Act in ways that made the Patriot Act seem more of a departure from existing law than it actually was. On reflection, today we can see that changes such as the pen register amendment did not substantially shift the balance between privacy and security. Rather, the law updated a 1986 privacy law and clarified that the same privacy protection that applies to the telephone also applies to the Internet. Much work remains to be done; the statutory laws that regulate Internet surveillance will surely keep Congress busy for years to come. However, the pen register amendments of the USA Patriot are best understood as part of a necessary response to preexisting ambiguities and technological change. They are consistent with rather than a departure from Congress's historical efforts to create rules that effectively balance privacy and security in new technologies.